UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/036,521	01/07/2002	Robert John Ackroyd	01.119.01	5107

7590 08/26/2005

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/036,521	ACKROYD, ROBERT JOHN	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 June 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's arguments/amendments with respect to amended claims 1-10, 13-15, 17-20, 22-24, and 27, presently pending claims 1-27, filed on June 02, 2005 have been fully considered but they are not persuasive. The examiner would like to point out that this action is made final (MPEP 706.07a).

2. The examiner accepts the amended drawings and 35 USC § 101 suggestions.

Response to Arguments

3. Applicant argues that:

a. Independent claims 1, 10, and 19 are not taught by neither of the references Schertz, Schnurer nor Chen alone or in combination to include *"a pattern of malware detection across said plurality of network connected computers, logging of data messages from which Applicant's invention detects the pattern, and also applicant argues that detection of a pattern of malware detection is not the detection of a virus"* (page 11 par. 2, page 12 par. 1-2, and page 13 par. 1).

b. The references, whether alone or in combination, fail to support wherein *"performing any action in response to the pattern detection, since there is no pattern detection disclosed by the references"* (page 11 par. 3).

c. Dependent claims 2-9, 11-18, and 20-27 are allowable based upon their dependency on allowable claims 1, 10, and 19 (page 12 par. 1).

However, Examiner disagrees with applicant.

Regarding argument (a), Argument is not persuasive. Schertz teaches detecting and reporting the presence of virus/worm (page 2 par. 0008). Detected virus signature pattern is compared with the predetermined/known virus signature pattern and action is taken if there is a match occurs (page 4 par. 0030 lines 9-10, page 3 par. 0022 lines 8-10, and page 2 par. 0018). Applicant is unclear about "virus signature". Virus signature is a bit of patterns and/or a pattern of malware (page 2 par. 0018 lines 7-10). Schertz teaches detecting from log data message. Predetermined/known virus signature patterns stored are compared with the newly detected virus pattern messages (page 4 par. 0030 lines 9-10, page 3 par. 0022lines 8-10, and page 2 par. 0018). Computer dictionary defines "Malware" as virus software. Malware is a generic term used to describe any form of malicious software that harms/destroys other software and/or networks. Example of malware includes Virus, Trojan horses, malicious active content, etc. Therefore detecting malware is detecting virus/worm across the network of connected computers (see, Schertz page 1 par. 0004; term virus includes any software code that act like a virus, worm, or any variant thereof).

Regarding argument (b), Argument is not persuasive. Schertz discloses performing actions in response of pattern detection. For example: discarding passing/transmitting

data to other network (page 3 par. 0020), closing communications on a port of the firewall to prevent delivery of the identified packets into the network (page 2 par. 0018), and reporting/notifying to the system administrator (page 4 par. 0030).

Regarding argument (c), examiner disagrees with applicant. Based on the arguments set forth by the examiner for arguments (a) and (b), the dependent claims stand rejected.

The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning. Therefore, the examiner asserts that the system of the prior art, Schertz, Schnurer, and Chen teach or suggest the subject matter as recited in independent claims 1, 10, and 19. Dependent claims 2-9, 11-18, and 20-27 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action dated August 12, 2005. Accordingly, rejections for claims 1-27 are respectfully maintained.

Rejections

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

5. Claims 1-3, 6-12, 15-21, and 24-27 are rejected under 35 U.S.C. 102(e) as being anticipated by Schertz et al. (Schertz, Pub. No.: US 2003/0084322 A1).

As per claims 1, 10, and 19, Schertz teaches a computer program product/method/apparatus for controlling a managing computer to manage malware protection within a computer network containing a plurality of network connected computers, said computer program product comprising:

receiving code operable to receive at said managing computer a plurality of log data messages identifying detection of malware by respective ones of said plurality of network connected computers (page 4 par. 0030 lines 9-10, and page 3 par. 0022 lines 8-10);

detecting code operable to detect from said plurality of log data messages received by said managing computer a pattern of malware detection across said plurality of network connected computers matching one or more predetermined trigger patterns (page 4 par. 0030 lines 9-21, page 3 par. 0021 lines 10-18, and par. 0023 lines 12-18); and

action performing code operable in response to detection of one or more predetermined trigger patterns to perform one or more predetermined anti-malware actions (page 4 par. 0030 lines 16-21, and page 3 par. 0020 lines 14-25).

As per claims 2, 11, and 20, Schertz teaches a computer program product/method/apparatus, wherein said plurality of network connected computers each have a malware scanner that serves to scan computer files to detected malware within said computer files (page 4 par. 0031 lines 1-3).

As per claims 3, 12, and 21, Schertz teaches a computer program product/method/apparatus,

wherein said malware scanner uses malware definition data to identify malware to be detected (page 4 par. 0031 lines 1-3, and fig. 1 No. 16).

As per claims 6, 15, and 24, Schertz teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include isolating one of more of said network connected computers from other parts of said computer network (page 4 par. 0031 lines 17-24 and page 3 par. 0020 lines 14-17).

As per claims 7, 16, and 25, Schertz teaches a computer program product/method/apparatus, wherein said managing computer stores said plurality of log data messages within a database (fig. 2 No. 80A and 81A).

As per claims 8, 17, and 26, Schertz teaches a computer program product/method/apparatus, wherein said detecting code is operable to query said database (page 18 lines 7-10).

As per claims 9, 18, and 27, Schertz teaches a computer program product/method/apparatus, wherein said database includes data identifying one or more of:

malware protection mechanisms used by respective network connected computers (page 2 par. 0016 lines 14-17);

versions of malware protection computer programs used by respective network connected computers (page 4 par. 0031 lines 1-3, and fig. 1 No. 16);

versions of malware definition data used by respective network connected computers (page 4 par. 0031 lines 1-3, and fig. 1 No. 16); and

security settings of malware protection mechanisms used by respective network connected computers (page 2 par. 0016 lines 14-17).

Claim Rejections - 35 USC § 103

6. Claims 4, 13, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schertz et al. (Schertz, Pub. No.: US 2003/0084322 A1) in view of Schnurer et al. (Schnurer, Patent Number: 5842002).

As per claims 4, 13, and 22, Schertz teaches all the subject matter as described above.
Schertz do not explicitly teach updating of malware definition data.
However Schnurer teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include forcing an update of malware definition data being used by one or more of said plurality of network connected computers (Schnurer col. 5 lines 16-19).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Schnurer within the system of Schertz because it would keep the detection device current (Schnurer col. 5 lines 16-19).

7. Claims 5, 14, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schertz et al. (Schertz, Pub. No.: US 2003/0084322 A1) in view of Chen et al. (Chen, Patent Number: 5,832,208).

As per claims 5, 14, and 23, Schertz teaches all the subject matter as described above. Schertz does not explicitly teach altering the scanner setting when malware is detected. However Chen teaches a computer program product/method/apparatus, wherein said one or more predetermined anti-malware actions include altering at least one scanner setting of at least one malware scanner such that said malware scanner performs more thorough malware scanning (Chen Fig. 3 No. 260; performing more thorough virus scanning after virus is detected).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Chen within the system of Schertz because it would scan the entire email/data to detect more virus if any.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Eleni Shiferaw
August 12, 2005

Primary Examiner
AU 2131
8/17/05